Procedia Computer Science

Volume 88, 2016, Pages 318–323

7th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2016

The design of integrity monitoring and reliability verification system for critical information, transmitted in automatic train signaling system, based on DMR-RUS radio channel

Valery Konyavskiy[1], Anna Epishkina[2] and Alexander Korotin[2]

[1]*Moscow Institute of Physics and Technology, Moscow, Russian Federation*

[2]*National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russian Federation*

Konyavskiy@gmail.com, avepishkina@mephi.ru, alexkor91@gmail.com

Abstract

This article gives us results of the work on ensuring protection of critical information, transmitted in automatic train signaling system (ALS), based on DMR-RUS radio channel (special version of Digital Mobile Radio for Russian railway), against computer attacks, targeted to modification and substitution of data. The purpose of this work is development of integrity monitoring and reliability verification system (IMRVS) for information, transmitted in ALS. There are different ways of building IMRVS. This article shows one of these methods, which, in authors' opinion, is optimal for using in ALS.

Keywords: automatic train signaling, transmission of critical information by radio channel, DMR-RUS, IMRVS

1 Introduction

Industrial control system (ICS) are widely used in the field of railway transport (RT). The application of ICS in RT allows solving such problems as planning and control of transportations, control and registration of the activity of enterprises and objects of railway sector and problems, related to the exploitation of railway infrastructure objects and their security [1].

The last class of problems, related to the exploitation of objects and their security, includes the problems of movement control of trains at stations and stages, control and diagnostics of locomotives, ensuring the security of trains' movement, control of electric power supply of railway infrastructure objects and others. It's necessary for the process of control of train's movement at stations and stages and ensuring of their security to use automatic train signaling systems (ALS), which are systems of transmission to locomotive onboard devices of information about permitted speed of movement and

Selection and peer-review under responsibility of the Scientific Programme Committee of BICA 2016

doi:10.1016/j.procs.2016.07.442

additional conditions of moving of railway rolling stock: speed limit, the route of moving at a railway station [2]. We will call the information transmitted with ALS critical information.

The traditional ALS, which uses track circuits [2], has some disadvantages. They are limited reliability, small information capacity of data transmitted to locomotive, a bigger measure of discreteness of determination of the train location [3]. The use of ALS system based on radio channel (GSM-R, DMR-RUS, Wi-Fi) allows to increase the speed at the sections of the track and throughput of stages by decreasing the amount of coding failures, optimization of speed modes and intervals of following trains.

Transition to the use of ALS based on radio channel leads to the appearance of a new class of security threats, associated with the disruption of transmitted data integrity by implementation of attacks on interception, modification and obtrusion of critical information when the perpetrator is far from the controlled zone (railway). The implementation of such attacks can lead to disturbance of train movement because of getting wrong critical information. At this moment ALS systems based on radio channel DMB-RUS don't have protection mechanisms against such attacks.

There is a contradiction – ALS systems based on radio channel DMR-RUS don't have necessary security mechanisms for integrity monitoring and reliability verification of critical information and at this moment there is no existing data protection tool for such type of ALS systems, which can implement these functions. The solution of this contradiction can become possible by designing integrity monitoring and reliability verification system of critical information [4], transmitted between the station and locomotive according to DMR-RUS Standard.

2 The description of DMR-RUS

Protocol DMR-RUS was based on Digital Mobile Radio Standard (DMR) [5]. The process of information exchange there is based on technology of Time Division Multiple Access (TDMA) and it consists of cycles of data transmission. Besides, information exchange is organized on the principle of "request-response", i.e. base radio station sends the request and subscriber's radio station replies it. Data transmission cycle consists of four frames, each frame has two time slots (Figure 1).

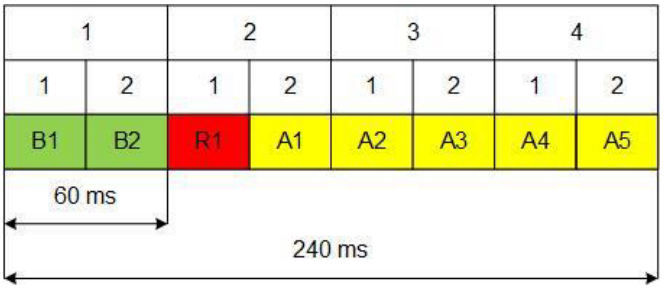

Figure 1: The structure of data transmission cycle in DMR-RUS

The data B1 and B2 of base station are being transmitted in the first and in the second time slots of the first frame. The first timeslot of the second frame is used for registration of new subscribers of the net (packet R1) or for sending a request of immediate transmission of data from subscriber's radio station. The second time slot of the second frame, the third and the fourth frames are used for transmitting data A1, A2, A3, A4, A5 of subscriber's radio station. Each packet of data B1, B2, R1, A1-A5 consists of 12 bytes.

2.1 Survey and registration of subscribers

Base radio station must make periodic survey and get data from registered subscribers. The periodicity of subscriber's survey is 2.88 seconds or 12 cycles. And besides there can be surveyed up to 12 subscriber's stations. In case of a big amount of subscribers on the net, the period of surveys increases.

To register a new subscriber's station, it sends a request for registration in the first time slot of the second frame (Figure 2). When the request was got the base radio station must send in B2 packet the ID of registering subscriber's radio station for its survey. Next in this cycle the registering subscriber's station must answer base station by sending packets A1-A5 (Figure 2). After that the registration is thought to be finished and the base station must begin the periodic survey of registered subscriber's radio station.

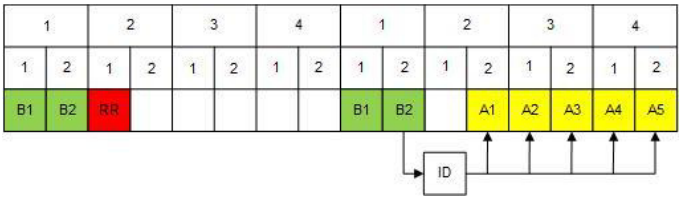

Figure 2: The scheme of subscriber's radio station registration

3 The design of IMRVS

Work model of ALS system based on DMR-RUS consists of two levels: application layer and data link layer. The exchange of critical information occurs at the application layer, or at the ALS layer, between the components of ALS system, installed at the station and at the locomotive. Data Link Layer, or radio station DMR-RUS layer, is responsible for critical information transfer between the base radio station, installed at a railway station, and subscriber's, installed on board of locomotive.

It is suggested for ensuring of integrity and reliability of transmitted information to develop additional layer of the model which would be located between the application and data link layers and which would provide the necessary level of protection (Figure 3). We'll call the suggested level the level of security, or the level of integrity monitoring and reliability verification (IMRVS). It is proposed that hardware and software components of IMRVS, installed at the station and locomotive, will exchange specially formed verification information, which confirms that critical information was received from legitimate station or locomotive.

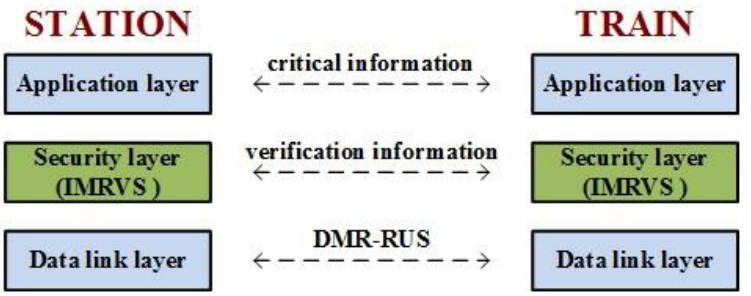

Figure 3: The proposed model of transmission of critical information by DMR-RUS

The achievement of the task set before IMRVS can become possible by using digital signature or authentication codes (MAC, HMAC) as verification information [4]. Moreover, because of the ability to use developing IMRVS at railway sections, which have federal significance, the protection mechanisms (digital signature or authentication codes) must be developed according to Russian State Standards and must use Russian cryptographic methods of information protection [6-8].

3.1 The requirements to IMRVS

During the designing of IMRVS it is necessary to consider functional requirements, imposed by the application layer, or ALS system, and also the limits of data link layer, associated with the particularities of DMR-RUS. These requirements and limits are:

1. The limit of transfer time of critical information. The minimum amount of data, which is necessary for ALS system's correct work, and relevant verification information must be transmitted by one period of survey (2.88 seconds).
2. The limit of DMR-RUS radio channel capacity. The amount of data, which can be transmitted from base radio station to registered subscribers by one whole period of survey, is equal to 192 bytes; from subscriber's radio station to base radio station this value is equal to 52 bytes.
3. The minimization of the amount of data security level. The amount of transmitted data of application layer by one period of survey depends on configuration of the station (the amount of ways, points, signals) and on the average is equal to 100 bytes during transferring from station to locomotive and 25 bytes in case of transferring data from locomotive to station. In this connection and considering the fact of possibility of further use of DMR-RUS radio channel not only in ALS system, the minimum size of verification information of security level is one of the main criteria during the development of IMRVS.
4. Broadcasting mode of the base radio station. As the base radio station transmits data to registered subscribers in broadcasting mode, the common key of verification of digital signature or authentication code must be used for all registered at the base radio station at the current moment locomotives for integrity monitoring and reliability verification of messages.

It should be noted that the problem of transferring the verification key to locomotive can be solved in three ways:

- Verification keys of all stations' messages are inserted into locomotives during the initial installation of IMRVS;
- Verification key is being transmitted to locomotive immediately at the moment of its registration at this station by DMR-RUS radio channel;
- Verification keys of stations' messages are transmitted to locomotive before train departure with additional communication channel (GSM, Wi-Fi) or external storage.

3.2 The proposed variant of building IMRVS

During the development of IMRVS we considered 6 variants of its building. Different variants of building are possible because of the choice of type of message verification (use of digital signature or authentication codes) and the way of transferring verification keys of station's messages to locomotive (The requirements to IMRVS). As a result of analysis of possible variants of building and fulfillment of the requirements described above, it is proposed to design IMRVS based on authentication codes with transmitting verification keys at the moment of locomotive's registration. The proposed structure of IMRVS is shown at Figure 4.

At the moment of registration the station transmits verification key Ks to locomotive. Next, the exchange of application layer data (ALD) between station and locomotive begins. The transmitted data is protected with the help of authentication codes (AC), generated on the key Ks. In case of mistake, ALS doesn't use received data and keeps waiting for the next message (similarly as in case when data wasn't delivered).

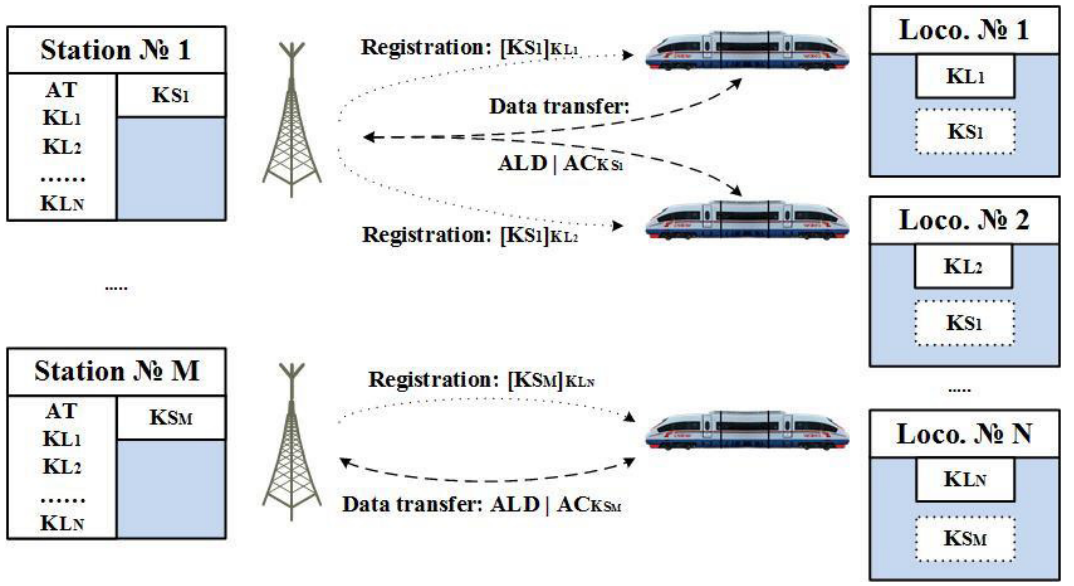

Figure 4: The proposed structure of IMRVS. AC is an authentication code; KS is a station key, which is used for generation and verification of AC; KL is a locomotive key, used for secure transfer of KS to locomotive; AT is an authenticity table, which contains all locomotive keys KL and which is stored at each station; ALD is application layer data; | means data concatenation; [ ]K means secure transfer with key K.

The process of registration of locomotive at the station and transferring message verification key Ks are shown at Figure 5. Locomotive sends IDi of its key K_{Li} with a random number R and AC for R on

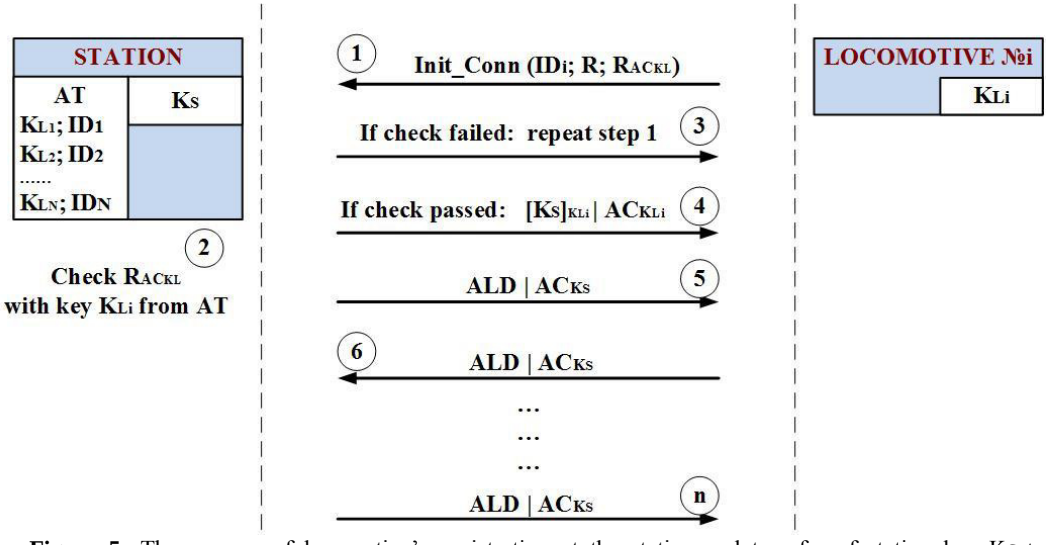

Figure 5: The process of locomotive's registration at the station and transfer of station key KS to locomotive. AC is an authentication code; KS is a station key which is used for generation and verification of AC ; KLi is a locomotive key, used for secure transfer of KS to locomotive; AT is an authenticity table, which contains all locomotive keys KL and which is stored at each station; IDi is the identifier of the ключа KLi at the AT; R is a random number; RACKL is an AC for R; ALD is an application layer data; | means data concatenation; [DATA]K means DATA encryption with key K.

the key K_{Li}. The station finds key K_{Li} with received IDi at authenticity table AT and verifies the received AC. If verification is failed, the station notifies locomotive about the necessity of the repetition of registration procedure. If verification is successful, the station sends to locomotive key Ks, encrypted on locomotive key K_{Li}, and adds generated with locomotive key AC to the end of the message. Locomotive verifies AC and in case of successful verification decrypts it and gets key Ks. After that the exchange of application layer data (critical information) begins.

4 Conclusion

As a result of this research, it is proposed to develop integrity monitoring and reliability verification system for transmitting critical information in ALS system, based on DMR-RUS radio channel. The relevance of such development can be explained by the lack of security mechanisms for such type of ALS systems. As a result of analysis of possible variants for building IMRVS and fulfillment of all requirements described above it was suggested to design IMRVS based on authentication codes with transmitting verification keys at the moment of locomotive's registration. The structure of suggested IMRVS was shown and the secure way of verification key transmitting at the registration moment was described in this article.

In future works it seems appropriate to develop final scheme of IMRVS, including key management, and to evaluate the possibility of the use of MAC or HMAC as authentication codes in IMRVS and to choose optimal variant.

5 Acknowledgements

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Professional Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

References

[1] Sankova G.V., Odudenko T.A. *Informatsionnyye tekhnologii v perevozochnom protsesse*. Khabarovsk, DVGUPS, 2012. (in Russian)

[2] GOST R 53431-2009. *Avtomatika i telemekhanika zheleznodorozhnaya. Terminy i opredeleniya*. (in Russian)

[3] Tilke I.G. ALS s ispolzovaniyem radiokanala. *Avtomatika, Svyaz, Informatika*. 2010, №7, c. 7-9. (in Russian)

[4] Konyavskiy V.A. *Upravleniye zashchitoy informatsii na baze SZI NSD «Akkord»*. Moscow, «Radio i svyaz», 1999. (in Russian)

[5] ETSI TS 102 361-(1-3). *Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) System.*

[6] GOST R 34.10-2012. *Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Protsessy formirovaniya i proverki elektronnoy tsifrovoy podpisi*. (in Russian)

[7] GOST R 34.11-2012. *Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Funktsiya kheshirovaniya*. (in Russian)

[8] GOST R 34.12-2015. *Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnyye shifry*. (in Russian)